UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/605,605	06/28/2000	Carl M. Ellison	042390.P7709	5805

7590 06/01/2004

William W Schaal
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	6

DATE MAILED: 06/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/605,605	ELLISON ET AL.
	Examiner	Art Unit
	Justin T. Darrow	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 15-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *12,15,21 and 22* is/are allowed.

6)☒ Claim(s) *1-11 and 16-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 have been presented for examination. Claims 11, 12, 16, 19 have been amended, claims 13 and 14 have been cancelled, and new claims 21 and 22 have been added in an amendment filed 03/18/2004. Claims 1-12 and 15-22 have been examined.

Response to Arguments

2. Applicant's arguments filed 03/18/2004 have been fully considered but they are not persuasive.

3. As per claims 1-12, the expression, $t_1{}^{v} (h\ h_i)^{t2}\ a$, (see Brands, page 11, step 2) represents the certificate template recited in independent claim 1. Additionally, hashing this value using blinded public key h_1' is represented by $H (h_1', t_1{}^{v} (h\ h_i)^{t2}\ a)$ to form a hash value c' (see Brands, page 11, step 2).

As per claims 16-20, the permanent key pair contains a pair consisting of a public key and matching certificate as a certified public key, and to a triple consisting of a secret key, a corresponding public key, and a matching certificate as a certified key pair (see page 8, section 2, paragraphs 2 and 3).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-12 and 16-20 are rejected under 35 U.S.C. 102(b) as being anticipated by S. Brands, "Restrictive Blinding of Secret-Key Certificates."

As per claim 1, Brands illustrates a method comprising:

producing a pseudonym including a public pseudonym key within a platform (see page 11, section 3.1, step 1 and figure 1; generating a public key, $a = w^v$);

placing the public pseudonym key into a certificate template (see page 11, section 3.1, step 2 and figure 1; placing a in $t_1^{\ v} (h\ h_i)^{t2}$ a);

performing a hash operation on the certificate template to produce a certificate hash value (see page 11, section 3.1, step 2 and figure 1; hashing this value using blinded public key h_1', $H(h_1', t_1^{\ v} (h\ h_i)^{t2} a)$ to form a hash value c');

performing a transformation on the certificate hash value for transmission from the platform (see page 11, section 3.1, step 2 and figure 1; transforming hash value c' into c);

receiving a signed result being a digital signature for the transformed certificate hash value (see page 11, section 3.1, step 3 and figure 1; performing an operation to form $r = (x\ y^{s0i})^c$ w and sending to R_i); and

performing an inverse transformation on the signed result to recover a digital signature of the certificate hash value (see page 11, section 3.1 and figure 1; performing an inverse transformation to recover a digital signature of the value c', r').

As per claim 2, Brands further depicts:

generating the public pseudonym key and a private pseudonym key corresponding to the

public pseudonym key (see page 11, section 3.1, step 1 and figure 1; that a and v are a public private key pair).

As per claim 3, Brands moreover shows:

writing the public pseudonym key into a field of the certificate template (see page 11, section 3.1, step 2 and figure 1; that a is written in $t_1{}^{v} (h\, h_i)^{t2}$ a).

As per claim 4, Brands then discusses:

performing a logical operation on the certificate hash value using a pseudo-random number to produce a value differing from the certificate hash value (see page 11, section 3.1, step 2 and figure 1; transforming hash value c' into c in $c = c' + t_2 \bmod v$, where $t_2 \bmod v$ is a random number).

As per claim 5, Brands also mentions:

that the pseudo-random number is a predetermined value raised to an inverse power designated by a pseudo-random value (see page 11, section 3.1, step 3; $r^{v} (h\, h_i)^{-c} = a$, where c is based on $t_2 \bmod v$, a random number).

As per claim 6, Brands further suggests:

that the pseudo-random value is stored in a secure memory (see page 11, section 3.1, steps 2 and 3, and figure 1; that R_i stores the pseudo-random value, $t_2 \bmod v$, after sending it to S, for subsequent computation).

As per claim 7, Brands next discusses:

performing a logical operation on the signed result using an inverse of the pseudo-random number (see page 11, section 3.1 and figure 1; the inverse transformation to recover the digital signature using the inverse of t_2 mod $r' = r\ t_1\ (\ h\ h_i\ )^{c' + t2\ div\ v}\ s_{1i}{}^{c'}$).

As per claim 8, Brands additionally points out:

digitally signing a certification request, including the transformed certificate hash value, with a private key of a first platform to produce a signed certification request (see page 11, section 3.1 and figure 1; signing the hash value with the private key s_{0i}, the private key of platform S).

As per claim 9, Brands then states:

obtaining a device certificate being a digital certificate chain that includes a public key of a first platform, to accompany the signed certificate request (see page 11, section 3.1, step 3 and figure 1; that the result includes the public key, y^{s0i}, $r = (x\ y^{s0i})^{c}\ w$).

As per claim 10, Brands also specifies:

transferring the signed certificate request and the device certificate to a second platform (see page 11, section 3.1, step 3 and figure 1; sending $r := (xy^{s0i})^{c}w$ to R_i).

As per claim 11, Brands further describes:

storing the digital signature of the certificate hash value for use in subsequent communications to a remotely located platform (see page 2, section 1, first full paragraph; the certificate for secure management of cryptographic keys).

As per claim 12, Brands describes a device with processing that contains a triple consisting of a secret key, a corresponding public key, and a matching certificate for a party to perform a cryptographic action (see page 8, section 2, paragraphs 2 and 3).

As per claim 13, Brands further specifies that this matching certificate as a certified key pair (see page 8, section 2, paragraph 3).

As per claim 15, Brands then discusses transforming hash value c' into c in $c = c' + t_2 \bmod v$, where $t_2 \bmod v$ is a random number (see page 11, section 3.1, step 2 and figure 1).

As per claim 16, Brands discloses a platform comprising:

a transceiver (see page 11, section 3.1; figure 1; S);

and a device in communication with the transceiver including a persistent memory (see page 11, section 3.1; figure 1; R) to contain

a permanent key pair (see page 8, section 2, paragraphs 2 and 3; which contains a pair consisting of a public key and matching certificate as a certified public key, and to a triple consisting of a secret key, a corresponding public key, and a matching certificate as a certified key pair) and

a digital signature of a hash value of a digital certificate chain that includes a public pseudonym key of the at least one pseudonym (see page 11, section 3.1 and figure 1; in which the certificate is a digital signature of a hash value of a digital certificate with a public key, $r = (x\ y^{s0i})^{c}\ w$).

As per claim 17, Brands further illustrates:

a processing unit (see figure 1; R with processing capability) to

(i) write the public pseudonym key into a certificate template (see page 11, section 3.1, step 2 and figure 1; placing a in $t_1^{v}\ (h\ h_i)^{t2}\ a$);

(ii) performing a hash operation on the certificate template to produce a certificate hash value (see page 11, section 3.1, step 2 and figure 1; hashing this value for form a hash value c'); and

(iii) performing a transformation operation of the certificate hash value (see page 11, section 3.1, step 2 and figure 1; transforming hash value c' into c).

As per claim 18, Brands additionally points out:

producing a digital signature of at least the transformed certificate hash value using a private key of the permanent key pair see page 11, section 3.1 and figure 1; signing the hash value with the private key s_{0i}).

As per claim 19, Brands also elaborates:

appending a device certificate with the digital signature of at least the transformed

certificate hash value (see page 11, section 3.1 and figure 1; the certificate, $r = (x\ y^{s0i})^{c}\ w$, includes the digital signature of the transformed certificate hash value, c).

As per claim 20, Brands then embodies:

that the device certificate is the digital certificate chain (see page 10, section 3, first paragraph; that the certificate of such a triple is uncorrelated to the view of the signer in the issuing protocol).

Allowable Subject Matter

6. Claims 12, 15, 21, and 22 are allowed.

7. The following is an examiner's statement of reasons for allowance:

8. Claims 12 and 15; and 21 and 22 are drawn to a device and method, respectively. The closest prior art, S. Brands, "Restrictive Blinding of Secret-Key Certificates," teaches a similar device and method. However, he neither shows nor implies erasing a second key pair after a communication session with the remotely located device has concluded (see page 8, section 2, paragraph 3). This particular feature explicitly recited in independent claims 12 and 21 renders claims 12 and 15; and 21 and 22, respectively, allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal

papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

June 1, 2004

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100